BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 31-7

2 MARCH 1993

Security

ACQUISITION SECURITY

OPR: HQ USAF/SPI (Mr Theodore Konduris)

Certified by: HQ USAF/SP
(Brig Gen Stephen C. Mannell)
Pages: 5
Distribution: F

1. Security for new weapon systems and technology is essential if the United States is to remain a military leader. Planning for and integrating security into the acquisition process is imperative to protect weapons systems and related sensitive technology from unauthorized disclosure, or sabotage, theft, or damage throughout a system's life cycle.

2. The Air Force will integrate security needs and requirements in a program protection plan (PPP) beginning in Phase 0 of an acquisition program. The Air Force will maintain this program's integrity throughout the acquisition process and system life cycle. For acquisition programs that are beyond Milestone I, the Air Force will develop and maintain a PPP to cover the remainder of the system's life.

3. The Air Force will apply System Security Engineering (SSE) by designing, engineering, and integrating security requirements into a weapon system and associated facilities throughout its life cycle.

4. The Air Force will apply Product Security (PRODSEC) by countering threats against sensitive resources located at contractor-owned or -operated facilities when other security rules do not provide the necessary protection.

5. Responsibilities and Authorities:

5.1. The Office of the Secretary of the Air Force and Headquarters US Air Force are responsible for policy, resource advocacy, and oversight of Air Force Acquisition Security. The Office of the Secretary of the Air Force, Management Policy and Program Integration (SAF/AQXA) is responsible for program protection planning policy. Headquarters US Air Force, Information Security (HQ USAF/SPI) advises SAF/AQXA on program protection planning policies impacting security police areas of responsibility. HQ USAF/SPI is responsible for SSE and PRODSEC policy. Headquarters Air Force Intelligence Support Agency, Security and Communications (HQ AFISA/INS) is responsible for managing Sensitive Compartmented Information (SCI) security programs under provisions of Director, Central Intelligence Directive 1/19. Headquarters US Air Force, C4 Plans and Policy (HQ USAF/SCX) is responsible for C4 systems security.

5.2. Operating commands are responsible for determining security needs and requirements throughout the acquisition process. They must work in conjunction with implementing, participating, and supporting command security specialists.

5.3. System program directors (SPD) are responsible for establishing acquisition security measures and guidance within their programs.

5.4. Servicing security police offices advise and assist system program directors in developing acquisition security plans.

6. Definitions:

6.1. Program Protection Planning (PPP). An acquisition program process that identifies a system's critical elements, threats, and vulnerabilities. The planning details how the Air Force will protect the system throughout its life cycle.

6.2. System Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify vulnerabilities. It also tries to reduce the number of actions necessary to eliminate or contain risks associated with security vulnerabilities.

6.3. Product Security (PRODSEC). Protection of sensitive government resources at contractor-owned or -operated facilities.

6.4. Eligible Acquisition Programs. Any acquisition program that is responsible for sensitive information in any form.

7. This policy implements Department of Defense Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, February 23, 1991, and MILSTD 1785, *Military Standard for System Security Engineering Program Management Requirements.*

8. This policy interfaces with various publications. Related policies are included in AFPD 10-6, *Mission Needs and Operational Requirements*; AFPD 31-4, *Information Security*; AFPD 31-5, *Investigations, Clearances, and Access Requirements*; AFPD 31-6, *Industrial Security*; USAFINTEL 201-1, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI)*, 1 May 1990 (copy available from the Supporting Security Office); and AFPD 33-2, *C4 Systems Security*. Related instructions are in AFI 31-701, *Program Protection Planning (PPP*); AFI 31-702, *System Security Engineering (SSE*) (formerly AFR 800-23); AFI 31-703, *Product Security (PRODSEC*); AFI 31-101; *Physical Security*; and AFI 31-209, *Resource Protection Program.*

9. See **Attachment 1** for the ways to measure compliance with this policy.

STEPHEN C. MANNELL, Brig General, USAF
Chief of Security Police

Attachment 1

MEASURING COMPLIANCE WITH POLICY

A1.1. Compliance with planning and integrating security in the acquisition process will be assessed by measuring the number of eligible acquisition programs that have or have not implemented Program Protection Planning; System Security Engineering; and Product Security. Each policy statement will be measured using a bar chart (**Figure A1.1.**, **Figure A1.2.**, and **Figure A1.3.**). Each bar chart will compare number of eligible acquisition programs against number implementing policy. Progress of acquisition programs implementing each policy statement will be shown over time. The desired outcome is that all eligible acquisition programs have implemented acquisition security.

A1.2. The measurement data will be provided by SPDs to HQ USAF/SPI via RCS: HAF-SPI(AR)9226. Twice a year, SAF/AQXA will send a survey to SPDs. SPDs will complete the survey and turn it in to their servicing security police office. The servicing security police office will send it to HQ USAF/SPI through AFMC/SP. HQ USAF/SPI will collect the data, consolidate it, and provide feedback to all security police and SPDs. Adjustments may have to be made to the surveys and measurements based on survey responses. These changes will be publicized with the feedback. Reporting will be discontinued during emergencies.

Figure A1.1. Sample Metric of Programs With Program Protection Planning.

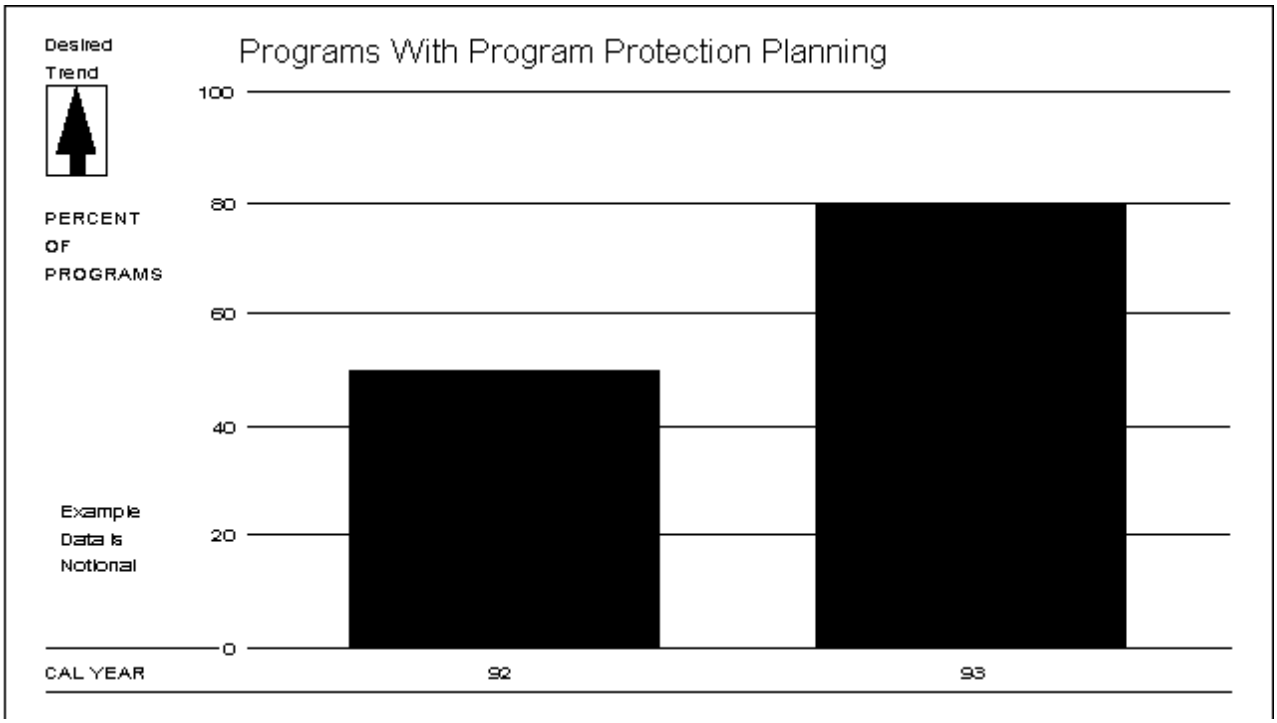

Figure A1.2. Sample Metric of Programs With Systems Security Engineering.

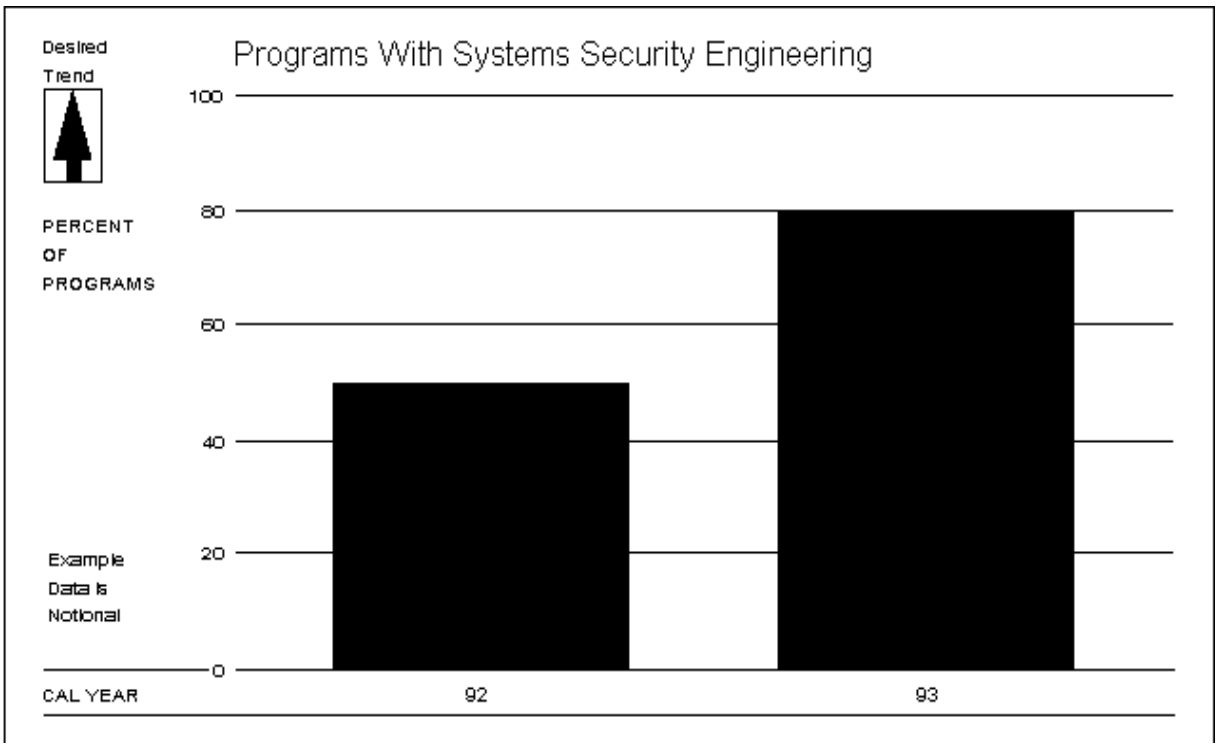

Figure A1.3. Sample Metric of Programs With Product Security.